AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the subject patent application.

Listing of Claims:

Claim 1 (Original): An encrypting device comprising:

key generation means for generating two prime numbers p and q of which product is n=pq as a private key and generating as a public key g1 and g2 respectively given by the following Equations (1) and (2) using two random numbers s and t and a maximal generator g in a multiplicative group of integers modulo n; and

encrypting arithmetic means for, in response to receipt of a plaintext m, generating a ciphertext C=(C1, C2) respectively given by the following Equations (3) and (4) using the public key {g1, g2}, a private key n, and random numbers r1 and r2,

$$g_1=g^{s(p-1)} \pmod n, \qquad (1)$$

$$g_2=g^{t(q-1)} \pmod n, \qquad (2)$$

$$C_1=m\cdot g_1^{r1} \pmod n, \qquad (3)$$

$$C_2=m\cdot g_2^{r2} \pmod n, \qquad (4)$$

where gcd{s, q-1}=1 and gcd{t, p-1}=1.

Claim 2 (Currently Amended): An encrypting device comprising:

key generation means for generating prime numbers p and q of which product is n=pq, where p is a private key, and generating as a public key g1 given by the following Equation (1) using a random number s and a maximal generator g in a multiplicative group of integers modulo n; and

encrypting arithmetic means for, in response to receipt of a plaintext m, generating a ciphertext C given by the following Equation (3)' using the public key g1, a private key n, and a random number r,

$$g_1=g^{s(p-1)} \pmod n, \qquad (1)$$

$$C=m \cdot g_1^{\,r} \pmod n, \qquad (3)'$$

where when ~~information~~ b is a size of p (bits), $0<m<2^{b-1}$ and $\gcd\{s, q-1\}=1$.

Claim 3 (Original): The encrypting device according to claim 1, wherein: e given by the following equation: e=h(d) (h is one-way hash function), where $d=(C_1+C_2)/m \pmod n$, is added to the ciphertext $C=(C_1, C_2)$ so as to be a ciphertext $C'=(C_1, C_2, e)$.

Claim 4 (Original): The encrypting device according to claim 1, further comprising:

a database for saving data resulting from calculation of a random number portion of the ciphertext C.

Claim 5 (Original): The encrypting device according to claim 1, wherein:

the encrypting arithmetic means encrypt only a plaintext element m1, which is a first element in the plaintext m, to the ciphertext element $C_1=(C_{11}, C_{12})$, and ciphertext elements following the ciphertext element C_1 are generated using a received plaintext m_i, bit information of the plaintext m_1, and two random numbers R_1 or R_2 which are contained in the ciphertext C_1.

Claim 6 (Original): A decrypting device wherein included are decrypting arithmetic means for receiving a ciphertext $C=(C_1, C_2)$, which is an encrypted plaintext m, respectively given by the following Equations (3) and (4) using a public key $\{g_1, g_2\}$,

a private key n, and random numbers r1 and r2, the private key n being n=pq where p and q are prime numbers generated as a private key, g1 and g2 being respectively given by the Equations (1) and (2) using two random numbers s and t and a maximal generator g in a multiplicative group of integers modulo n, and

performing decryption in such a manner so as to generate received ciphertexts a and b respectively given by the following Equations (5) and (6) using the Fermat's little theorem and then derive the plaintext m satisfying the following Equation (7) from the received ciphertexts a and b using the Chinese remainder theorem,

$$g_1=g^{s(p-1)} \pmod n, \quad (1)$$

$$g_2=g^{t(q-1)} \pmod n, \quad (2)$$

$$C_1=m\cdot g_1^{r1} \pmod n, \quad (3)$$

$$C_2=m\cdot g_2^{r2} \pmod n, \quad (4)$$

$$a=C_1 \pmod p)=m \pmod p), \quad (5)$$

$$b=C_2 \pmod q)=m \pmod q), \quad (6)$$

$$m=aAq+bBp \pmod n), \quad (7)$$

where $\gcd\{s, q-1\}=1$, $\gcd\{t, p-1\}=1$, $Aq \pmod p)=1$, and $Bp \pmod q)=1$.

Claim 7 (Original): A decrypting device wherein included are decrypting arithmetic means for receiving a ciphertext C of an inputted plaintext m, given by the following Equation (3)' using a public key g1, a private key n, and a random number r, the private key n being n=pq where p and q are prime numbers, p being generated as a private key, g1 being given by the following Equation (1) using a random number s and a maximal generator g in a multiplicative group of integers modulo n, and

performing decryption in such a manner so as to derive the plaintext m satisfying the following Equation (8) using the Fermat's little theorem,

$$g_1=g^{s(p-1)} \pmod n, \quad (1)$$

$$C=m\cdot g_1^{r} \pmod n, \quad (3)'$$

$$m=C \pmod p), \quad (8)$$

where $\gcd\{s, q-1\}=1$.

Claim 8 (Original): A cryptosystem comprising:

an encrypting device including: key generation means for generating two prime numbers p and q of which product is n=pq as a private key and generating as a public key g1 and g2 respectively given by the following Equations (1) and (2) using two random numbers s and t and a maximal generator g in a multiplicative group of integers modulo n; and encrypting arithmetic means for, in response to receipt of a plaintext m, generating a ciphertext $C=(C_1, C_2)$ respectively given by the following Equations (3) and (4) using the public key $\{g_1, g_2\}$, a private key n, and random numbers r1 and r2; and

a decrypting device including decrypting arithmetic means for receiving ciphertext elements C_1 and C_2 calculated by the encrypting device and performing decryption in such a manner so as to generate received ciphertexts a and b respectively given by the following Equations (5) and (6) using the Fermat's little theorem and then derive the plaintext m satisfying the following Equation (7) from the received ciphertexts a and b using the Chinese remainder theorem,

$$g_1=g^{s(p-1)} \pmod{n}, \qquad (1)$$
$$g_2=g^{t(q-1)} \pmod{n}, \qquad (2)$$
$$C_1=m\cdot g_1^{r1} \pmod{n}, \qquad (3)$$
$$C_2=m\cdot g_2^{r2} \pmod{n}, \qquad (4)$$
$$a=C_1 \pmod{p}=m \pmod{p}, \qquad (5)$$
$$b=C_2 \pmod{q}=m \pmod{q}, \qquad (6)$$
$$m=aAq+bBp \pmod{n}, \qquad (7)$$

where $\gcd\{s, q-1\}=1$, $\gcd\{t, p-1\}=1$, $Aq \pmod{p}=1$, and $Bp \pmod{q}=1$.

Claim 9 (Original): A cryptosystem comprising:

an encrypting device including: key generation means for generating prime numbers p and q of which product is n=pq, where p is a private key, and generating as a

public key g1 given by the following Equation (1) using a random number s and a maximal generator g in a multiplicative group of integers modulo n; and encrypting arithmetic means for, in response to receipt of a plaintext m, generating a ciphertext C given by the following Equation (3)' using the public key g1, a private key n, and a random number r; and

a decrypting device including decrypting arithmetic means for receiving the ciphertext C from the encrypting device and performing decryption in such a manner so as to derive the plaintext m satisfying the following Equation (8) using the Fermat's little theorem,

$$g_1=g^{s(p-1)} \pmod n, \qquad (1)$$

$$C=m\cdot g_1^{\,r} \pmod n, \qquad (3)'$$

$$m=C \pmod p, \qquad (8)$$

where $\gcd\{s, q-1\}=1$.

Claim 10 (Original): An encrypting method comprising the steps of:

generating two prime numbers p and q of which product is n=pq as a private key and generating as a public key g1 and g2 respectively given by the following Equations (1) and (2) using two random numbers s and t and a maximal generator g in a multiplicative group of integers modulo n; and

in response to receipt of a plaintext m, generating ciphertext elements C1 and C2 respectively given by the following Equations (3) and (4) using the public key $\{g_1, g_2\}$, a private key n, and random numbers r1 and r2,

$$g_1=g^{s(p-1)} \pmod n, \qquad (1)$$

$$g_2=g^{t(q-1)} \pmod n, \qquad (2)$$

$$C_1=m\cdot g_1^{\,r1} \pmod n, \qquad (3)$$

$$C_2=m\cdot g_2^{\,r2} \pmod n, \qquad (4)$$

where $\gcd\{s, q-1\}=1$ and $\gcd\{t, p-1\}=1$.

Claim 11 (Currently Amended): An encrypting method comprising the steps of:

generating prime numbers p and q of which product is n=pq, where p is a private key, and generating as a public key g_1 given by the following Equation (1) using a random number s and a maximal generator g in a multiplicative group of integers modulo n; and

in response to receipt of a plaintext m, generating a ciphertext C given by the following Equation (3)' using the public key g_1, a private key n, and a random number r,

$$g_1 = g^{s(p-1)} \pmod{n}, \qquad (1)$$

$$C = m \cdot g_1^{\,r} \pmod{n}, \qquad (3)'$$

where when ~~information~~ b is a size of p (bits), $0<m<2^{b-1}$ and $\gcd\{s, q-1\}=1$.

Claim 12 (Original): A decrypting method comprising the steps of:

receiving a ciphertext $C=(C_1, C_2)$, which is an encrypted plaintext m, respectively given by the following Equations (3) and (4) using a public key $\{g_1, g_2\}$, a private key n, and random numbers r1 and r2, the private key n being n=pq where p and q are prime numbers generated as a private key, g_1 and g_2 being respectively given by the Equations (1) and (2) using two random numbers s and t and a maximal generator g in a multiplicative group of integers modulo n; and

performing decryption in such a manner so as to generate received ciphertexts a and b respectively given by the following Equations (5) and (6) using the Fermat's little theorem and then derive the plaintext m satisfying the following Equation (7) from the received ciphertexts a and b using the Chinese remainder theorem,

$$g_1 = g^{s(p-1)} \pmod{n}, \qquad (1)$$

$$g_2 = g^{t(q-1)} \pmod{n}, \qquad (2)$$

$$C_1 = m \cdot g_1^{\,r1} \pmod{n}, \qquad (3)$$

$$C_2 = m \cdot g_2^{\,r2} \pmod{n}, \qquad (4)$$

$$a = C_1 \pmod{p} = m \pmod{p}, \qquad (5)$$

$b=C_2 \pmod{q}=m \pmod{q}$, (6)

$m=aAq+bBp \pmod{n}$, (7)

where $\gcd\{s, q-1\}=1$, $\gcd\{t, p-1\}=1$, $Aq \pmod{p}=1$, and $Bp \pmod{q}=1$.

Claim 13 (Original): A decrypting method comprising the steps of:

receiving a ciphertext C of an inputted plaintext m, given by the following Equation (3)' using a public key g_1, a private key n, and a random number r, the private key n being n=pq where p and q are prime numbers, p being generated as a private key, g_1 being given by the following Equation (1) using a random number s and a maximal generator g in a multiplicative group of integers modulo n; and

performing decryption in such a manner so as to derive the plaintext m satisfying the following Equation (8) using the Fermat's little theorem,

$g_1=g^{s(p-1)} \pmod{n}$, (1)

$C=m \cdot g_1^{\,r} \pmod{n}$, (3)'

$m=C \pmod{p}$, (8)

where $\gcd\{s, q-1\}=1$.